

REMARKS/ARGUMENTS

1.) Claim Amendments

The Applicant has amended claims 1, 8-9 and 19-22. Applicant respectfully submits no new matter has been added. Accordingly, claims 1-12 and 19-22 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

2.) Claim Rejections – 35 U.S.C. § 112

Claims 1-12 stand rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter as the invention. Claims 1 and 8 have been amended to correct the antecedent basis problem in each claim. The remaining claims, are rejected because of their dependency on rejected claims 1 and 8. The Applicants have corrected the deficiencies in claims 1 and 8 and the Applicants respectfully submit that remaining dependent claims are now allowable.

3.) Claim Rejections – 35 U.S.C. § 103 (a)

Claims 1-5, 7-9 and 19-20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Ziliacus, *et al.* (US 6,915,272) in view of Tabuki (US 5,841,970).

Claims 10-11 and 21-22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Ziliacus, *et al.* (US 6,915,272) in view of Tabuki (US 5,841,970) in view of Dang (US 20030101113) and further in view of Honjo (US 20020049912).

Claim 1 has been amended to claim as follows:

A method of communicating data securely within a wireless communications network, comprising the steps of:

maintaining a database server and a separate authentication server;

storing information and an associated data record within said database server, said information adapted to being accessed by a mobile station, said information having been encrypted using a data access key;

maintaining said data access key within said authentication server;

transmitting, by said mobile station, a first authentication request to

said authentication server;
 receiving said first authentication request at said authentication server from said mobile station;
 providing a first key from said authentication server to said mobile station in response to said first authentication request;
 receiving a second authentication request at said authentication server from said database server, said second authentication request further including said first key provided by said authentication server to said mobile station and a particular data identifying said information to which said mobile station is requesting access;
 determining at said authentication server as to whether said mobile station has authority to access said particular database record; and
 in response to an affirmative determination,
 instructing said database server to provide information associated with said requested database record to said mobile station; and
 providing by said authentication server to said mobile station a second key enabling said mobile station to decrypt said information received from said database server using said second key.

Claim 8 has been amended to claim as follows:

A method of storing and communicating data securely within a mobile telecommunications network wherein said mobile telecommunications network provides wireless service to a wireless device and further includes an authentication server and a separate database server, comprising the steps of:

 storing particular information within said database server wherein said information and an associated data record is stored encrypted using a first encryption key;

 communicating, by [[a]] said wireless device, separately with [[an]] said authentication server and said database server;

 receiving a request from said wireless device to access said information within said database server;

 in response to said request, transmitting an authentication request from said database server to said authentication server;

 receiving authentication approval, by said database server, from said authentication server regarding said wireless device for said information;

 further providing, by said authentication server a decryption key to said wireless device; and

 providing, by said database server, said requested information encrypted to said wireless device wherein said wireless device decrypts

said information using said decryption key provided by said authentication server.

Claim 19 has been amended to claim as follows:

A mobile communications network for storing and communicating data securely with a wireless device, comprising:

- a database server;
- an authentication server;
- a means for storing particular information within said database server, said information adapted to being accessed by said wireless device, wherein said data is stored encrypted using a first encryption key;
- a means for receiving a request for information by from said wireless device to access said stored information within said database server;
- a means for transmitting an authentication request to said authentication server in response to said request for information;
- a means for receiving authentication approval from said authentication server regarding said wireless device for said requested information wherein said authentication server further providing an decryption key to said wireless device; and
- a means for providing said requested information encrypted to said wireless device wherein said wireless device decrypts said information using said decryption key provided by said authentication server.

Applicant respectfully submits that the cited references, either alone or in combination, do not disclose, teach or suggest a mobile station communicating separately with an authentication server and a database server as recited in amended independent claims 1, 8 and 19.

In rejecting claims 1, 8, 9, 19 and 20, the Examiner cites col. 6, lines 20-45 of Zilliacus (See page 4 of the Office Action) for disclosing the steps of communication between a mobile station and an authentication server and between a mobile station and a database server, wherein a first key is provided from the authentication server to the mobile station in response to an authentication request:

Referring to FIG. 2, authentication in a GSM network is performed by the generation of a signed response (SRES) 150 by both the mobile station (MS) 10 and the telecom infrastructure 70 which is a function of a unique secret key (Ki) 110 of the mobile station 10 and a random number

(RAND) 150. The signed response (SRES) 150 is calculated in a subscriber identification module (SIM) (not shown) located in the mobile station (MS) 10, based on Ki 110 inside the SIM and RAND 140 obtained from the network authentication center (AuC) (not shown) in the telecom infrastructure 70. Additionally, the mobile station (MS) 10 and the telecom infrastructure 70 each perform encryption by generating a ciphering key (Kc) 100 which is a function of the same random number RAND 140 and the secret key (Ki) 110 of the mobile station 10. This authentication algorithm is a two stage process described in detail ahead in reference to FIG. 3 and FIG. 4 which employs two authentication algorithms. The first authentication algorithm, which calculates SRES 150, is known as the A3 algorithm module 120 and the second algorithm which computes Kc 100, which is computed each time a mobile station is authenticated, is known as the A8 algorithm module 130. However, each of the operations of authentication and computing of the ciphering key (Kc) 110 requires the mobile station (MS) 10 to be programmed to perform the aforementioned computations.

Notably, the above description only discloses the process by which a mobile station is authenticated for use in a communications network. It does not disclose accessing data from a database server by a mobile station/wireless device or the process of authentication of a mobile station/wireless device for the purpose of accessing by the mobile station/wireless device encrypted information on a database server. Thus, the first elements of claims 1, 8 and 19 are not disclosed by Zilliacus. Examiner further cites col. 9, line 60 through col. 10, line 31 for the elements of the second authentication request between a database server and an authentication server including the first key and data about the data record for which the mobile station is requesting access:

Referring to FIG. 7, the business model B 1200 begins execution in operation 460 by the user or consumer visiting, for example, a web site of a content provider 30 where he orders a content 50 item, such as a new game. In operation 470, the content provider 30 sends the user a random number (RAND) 140. The user computes a first SRES 150 using A3 algorithm module 120 and Kc 100 using A8 algorithm 130 and sends SRES 150 back to the content provider 30, together with his mobile network identifier. This mobile network identifier may include a location area identity (LAI) and Temporary Mobile Subscriber Identity (TMSI). However, the user may also supply the content provider 30 with an alias

which the network operator 20 may use to lookup the mobile network identifier. In operation 480, the content provider 30 sends the content identifier, CID, the mobile network identifier and the pair (RAND 140, SRES 150) to the network operator 20. Thereafter in operation 490, the network operator 20 computes a second SRES 150 and Kc 100 from RAND 140 using A3 algorithm module 120 and A8 algorithm module 130. This calculation is based on the secret key Ki 110 that is stored in the authentication center AuC that is part of the telecom infrastructure 70. In operation 500, a determination is made if the computed value of SRES 150 is the same as the value received from the content provider 30. If the two do not match then processing proceeds to operation 510 where a negative response is sent to the content provider 30. If the two SRES 150 values do match, then processing proceeds to operation 520. In operation 520, the network operator 20 charges the user or consumer for the content 50 and transmits a positive acknowledgment containing the key Kc 100, which enables content provider 30 to encrypt the content 50. Thereafter, in operation 530, the content provider 30 sends the content 50 to the user or consumer encrypted based on Kc 100. The content provider 30 then stores the triplet (CID, RAND 140, SRES 150) in his database. This stored triplet serves as proof that a user or consumer having the capability of computing SRES 150 from RAND 140 has been charged by the network operator 20 for the content 50 identified by the CID.

It is first noted that each of the elements of independent claims 1, 8 and 19 were not mapped to a corresponding element of Zilliacus. Had such mapping been done, it would be clear that the above description of Zilliacus does not disclose the second set of elements of claims 1, 8 and 19 of the present invention. For example, in the present invention, the database server (equated to the content provider of Zilliacus) further communicates with the authentication server in authenticating the mobile station/wireless device (equated to the user of Zilliacus) before sending the information requested by the mobile station from the database server. Yet, in contrast, the second line above provides: ".In operation 470, the content provider 30 sends the user a random number (RAND) 140." From the RAND, the user generates a key which is sent back to the content provider. No such actions are required by the present invention when authenticating a mobile station to access encrypted information on a database server. Further, Zillacus does not disclose the steps/components of the present invention used in authenticating the mobile station/wireless device which are arranged in the manner disclosed in the present invention. Zilliacus relies on the Global System

for Mobile (GSM) communications system to authenticate a user and provide algorithms and modules that are used to generate cipher keys and service responses so as to insure a content provider will be paid and that the user will not be overcharged. These algorithms and modules are used to encrypt information so as to prevent third parties from intercepting this important information. However, Ziliacus relies on communications between the user and content provider in authenticating the user. These are not equivalent to the authentication process that occurs in the present invention wherein such communications occur between the database server and the authentication server. When the content provider of Ziliacus is equated to the database server of the present invention, and the user with the mobile station/wireless device, it is clear that the process of the present invention is qualitatively different from that disclosed by Ziliacus.

Examiner further cites Tabuki as disclosing a single authentication server system. Tabuki discloses a client, an application server and a verification. The client sends authentication data to the application server, which verifies the authentication data by forwarding the authentication data to a verification server for authentication. However, Tabuki does not cure the deficiencies described above with respect to Ziliacus. Tabuki, does not disclose, alone or in combination with Ziliacus, the elements of independent claims 1, 8 and 19 as discussed above.

Examiner further cites Takamoto with respect to the information updating elements of claims 6 and 12, and Dang on Honjo with respect to the use of a session key being generated by the authentication server of claims 10-11 and 21-22.

Takamoto discloses a means by which a user transmits, from an on-premises terminal or an off-premises terminal, his/her user ID and password as well as an address of a web page that the user attempts to access. A login authentication apparatus receives them and determines whether the received user ID, password and address of the web page match any of those stored in an authentication table within its master file. If they match, the login authentication apparatus transmits the address of the web page to a proxy server, so that the user is allowed to access the desired web page. In contrast, in claims 1, 8 and 19, the authentication key is communicated

between a database server and authentication server. In Takamoto, the web page server does not participate in the key exchange.

In Dang, an infrastructure for an intelligent, program controlled apparatus, a system, a service and a method for identifying taxable financial transactions, collecting data based on the transactions, calculating any tax due on the transactions, reporting the same to a selected government authority, and periodically remitting funds corresponding to the taxes owed to the government authority over an interactive communications network, e.g., the Internet, an intranet, an extranet, or the like is disclosed. Paragraph [00016] of Dang provides:

Another embodiment of the present invention relates to a method for preventing entry of unwanted data to a system for providing financial data computation, report remittance and funds transfer services over an interactive communications network. First, a transaction request is received from a network browser of a subscriber server. The request is parsed for data that includes a session key encrypted using the subscriber server's public key to a service provider server. If the session key is located, then the transaction request is approved for entry to the system, and is sent to the service provider server.

Dang is a business method patent. Even assuming that a session key is sent by a subscriber to a server, Dang does not disclose the key exchange and authentication process described in the present invention. Specifically, Dang does not disclose communications between an authentication server and database server that is used to authenticate a subscriber to access information on a database server.

Honjo discloses an access control method for use with a system including a client, an Internet server, and a ticket granting server. The Internet server has a server policy defining an access allowance condition and sends a server policy to the client having requested an access. The ticket granting server obtains, in response to a request and the server policy sent from the client, personal information from a personal information database, authenticates the personal information, and sends it as a ticket to the client. The client sends an access request with the ticket to the Internet server. The Internet server allows the client the access when the ticket matches the server policy.

Honjo discloses, in effect, authentication by a ticket server (authentication server) by which a ticket (session key) is sent to the client (mobile station/wireless device) that is then used by the client to send an access request, with the ticket, to an Internet server (database server). Hence, even if the ticket of Honjo is equated with a session key, it can be clearly seen, that the method of Honjo is entirely different from that claimed in the present invention.

As noted, none of these additional references cure the deficiencies cited above with respect to Zilliacus. None of Takamoto, Dang nor Honjo disclose, alone or in combination with Zilliacus and Tabuki, all of the elements of independent claims 1, 8 and 19.

Claims 2-7 depend from amended claim 1 and recite further limitations in combination with the novel elements of claim 1. Claims 9-12 depend from amended claim 8 and recite further limitations in combination with the novel elements of claim 8. Claims 20-22 depend from amended claim 19 and recite further limitations in combination with the novel elements of claim 19. Therefore, the allowance of claims 1-12 and 19-22 is respectfully requested.

4.) Prior Art Not Relied Upon

In paragraph 14 on page 9 of the Office Action, the Examiner stated that the prior art made of record and not relied upon is considered pertinent to the Applicant's disclosure. None of the references alone or in combination, identically disclose the present invention.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,



Michael Cameron
Registration No. 50,298

Date: January 9, 2007

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-4145
mike.cameron@ericsson.com